UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/608,831	06/30/2000	Srinath Gundavelli	50325-0127	1955

29989 7590 08/25/2004

HICKMAN PALERMO TRUONG & BECKER, LLP
1600 WILLOW STREET
SAN JOSE, CA 95125

EXAMINER	
CURCIO, JAMES A F	

ART UNIT	PAPER NUMBER
2122	9

DATE MAILED: 08/25/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/608,831	GUNDAVELLI ET AL.	
	Examiner	Art Unit	
	James Curcio	2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *03 May 2004*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *53* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-53* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Response to Arguments

1. Applicant's arguments filed on May 3, 2004 have been fully considered but they are not persuasive.

In remarks regarding the rejection of claim 1, recapitulated for claims 2-33, Applicant seems to rely on an overly narrow interpretation of the claim language "based on" in the feature "computing a second secret key based on the first user exchange key and the first shared secret key" to overcome rejection. Applicant cites examples of how, in the preferred embodiments of the invention, the computation of a second secret key is based on or depends on the first user exchange key and the first shared secret key. However, neither the Applicant's claim language nor the specification limits the "based on" relationship to the preferred embodiments' enablement of the relationship.

The Examiner uses the broadest reasonable interpretation of the phrase "based on" in the feature "computing a second secret key based on the first exchange key and the first shared secret key." This interpretation includes all ways in which the second secret key's computation can be based on the first exchange key and the first shared key. Under this broadest reasonable interpretation, the existence of the first exchange key and the first shared key can serve as the basis.

The art applied in the rejection of claim 1--- Wechselberger – abstract and Hardjono – abstract, col. 3:10-26, and figure 5 - element 505 --- read on at least this basis, as required by claims 1-33. Therefore, claim 1 remains rejected.

Further limitations of this feature and other features pointed out in the Applicant's dependent claims are read upon as before by the art applied in the rejections of the previous Office Action. Therefore, claims 2-33 also remain rejected.

The outstanding rejections in the previous Office Action, with added consideration of claims 34-53, are repeated below.

Claim Rejections - 35 USC § 102

2. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

3. Claims 1, 10, 19, 28, 34-42, and 51-53 rejected under 35 U.S.C. 102(b) as being anticipated by Wechselberger et al (4531020).

4. As per claims 1, 10, 19, and 28, Wechselberger et al discloses a step for computing a first shared secret key (abstract), a generating step (abstract), a receiving step (abstract), a step for computing a second secret key (abstract), a sending step (abstract), and an establishing step (abstract).

5. As per claims 34-42 and 51-53, in addition to the teachings applied above, Wechselberger et al discloses that the first user exchange key is received by a particular member ... that the particular first member sends the first user exchange key

to the other first members of the set of one or more first members, that the other first members of the set of one or more first members receive the first user exchange key, that each first member of the set of one or more first members computes the second secret key.... that the set of one or more first members is a set of one or more first workstations, and that the first user is a second workstation (abstract; col. 3:28-68; and col. 4:25 to col. 5:66).

6. Claims 1, 10, 19, 28, 34-42, and 51-53 rejected under 35 U.S.C. 102(e) as being anticipated by Hardjono (US6584566B1).

7. As per claims 1, 10, 19, and 28, Hardjono discloses a step for computing a first shared secret key (abstract; column 3, lines 10-26; and figure 5, element 505), a generating step (abstract; column 3, lines 10-26; and figure 5, element 530), a receiving step (abstract; column 3, lines 10-26; and figure 5, element 530), a step for computing a second secret key (abstract; column 3, lines 10-26; and figure 5, element 505), a sending step (figure 5, element 530), and an establishing step (abstract; column 3, lines 10-26; and figure 5, elements 525 and 530).

8. As per claims 34-42 and 51-53, in addition to the teachings applied above, Hardjono discloses that the first user exchange key is received by a particular member ... that the particular first member sends the first user exchange key to the other first members of the set of one or more first members, that the other first members of the set of one or more first members receive the first user exchange key, that each first member of the set of one or more first members computes the second secret key.... that the set of one or more first members is a set of one or more first workstations, and

that the first user is a second workstation (abstract; col. 3:10-26; and figure 5-elements 505 and 530 and associated text).

Claim Rejections - 35 USC § 103

9. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

10. Claims 7, 16, 25, and 48 rejected under 35 U.S.C. 103(a) as being unpatentable over Hardjono (US6584566B1). Hardjono discloses a step for computing a first shared secret key (abstract; column 3, lines 10-26; and figure 5, element 505), a generating step (abstract; column 3, lines 10-26; and figure 5, element 530), a receiving step (abstract; column 3, lines 10-26; and figure 5, element 530), a step for computing a second secret key (abstract; column 3, lines 10-26; and figure 5, element 505), a sending step (figure 5, element 530), and an establishing step (abstract; column 3, lines 10-26; and figure 5, elements 525 and 530). Hardjono fails to expressly disclose the generation of a second multicast group exchange key, the reception of a second user exchange key, the computation of a third secret key, the sending of the second multicast group exchange key, and the establishment of a third multicast group. However, these steps are a reapplication in exact form of five steps in Hardjono listed and referenced above. Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify Hardjono by reapplying the generation, reception, computation, sending, and establishment steps. One of ordinary

skill in the art would have been motivated to do so in order to add a new member to the set of clients to whom data is multicast.

11. Claims 6, 15, 24, and 47 rejected under 35 U.S.C. 103(a) as being unpatentable over Hardjono (US6584566B1) as applied to claims 1, 10, 19, and 28 above, and further in view of Aziz (US6330671B1). In addition to the teachings applied above, while Hardjono fails to expressly disclose a verifying step and providing step, Aziz teaches these steps (Aziz – abstract). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify Hardjono by verifying against an authenticated predetermined list of clients having permission to receive a cryptographic key a client requesting multicast data and by providing this client with this key if the client is on the list as per the teachings of Aziz. One would have been motivated to do so in order to provide a secure key management system (Aziz – abstract).

12. Claims 2-5, 11-14, 20-23, 29-31, and 43-46 rejected under 35 U.S.C. 103(a) as being unpatentable over Hardjono (US6584566B1) as applied to claims 1, 10, 19, and 28 above, and further in view of Koblitz.

13. As per claims 2-5, 11-14, 20-23, 29-31, and 43-46, in addition to the teachings applied above, while Hardjono fails to expressly disclose the mathematical relations involved in the steps for computing a first shared secret key, generating a first multicast group exchange key, receiving a first user exchange key, and sending the first multicast group exchange key, Koblitz teaches these relations in his discussion of modular exponentiation by the repeated squaring method (Koblitz – page 23). Therefore, it

would have been obvious to one of ordinary skill in the art at the time the invention was made to modify Hardjono by using the repeated squaring method to compute the first shared secret key, generate a first multicast group exchange key, receive a first user exchange key, and send the first multicast exchange key as per the teachings of Koblitz. One would have been motivated to do so in order to quickly create the keys in these steps (Koblitz – page 23).

14. Claim 32 rejected under 35 U.S.C. 103(a) as being unpatentable over Hardjono (US6584566B1) as applied to claims 1, 10, 19, and 28 above, and further in view of Aziz (US6330671B1) and Koblitz. In addition to the teachings applied above, while Hardjono fails to expressly disclose a verifying step, a providing step, and the mathematical relations involved in the steps for computing a first shared secret key and generating a first multicast group exchange key, Aziz teaches the verifying and providing steps (Aziz – abstract) and Koblitz teaches the mathematical relations in his discussion of modular exponentiation by the repeated squaring method (Koblitz – page 23). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify Hardjono by verifying against an authenticated predetermined list of clients having permission to receive a cryptographic key a client requesting multicast data and by providing this client with this key if the client is on the list as per the teachings of Aziz and by using the repeated squaring method to compute the first shared secret key and to generate a first multicast group exchange key as per the teachings of Koblitz. One would have been motivated to do so in order to provide a

secure key management system (Aziz – abstract) and to quickly create the keys in the computing and generating steps (Koblitz – page 23).

15. Claims 9, 18, 27, and 50 rejected under 35 U.S.C. 103(a) as being unpatentable over Hardjono (US6584566B1) as applied to claims 1, 10, 19, and 28 above, and further in view of Srivastava (US6684331B1). In addition to the teachings applied above, while Hardjono fails to expressly disclose that the establishing step requires a total of approximately N+1 messages, Srivastava teaches this requirement (Srivastava – abstract). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made by modifying Hardjono by including this requirement as per the teaching of Srivastava. One of ordinary skill in the art would have been motivated to do so in order to establish secure and efficient multicast communication (Srivastava – abstract).

16. Claims 8, 17, 26, 33, and 49 rejected under 35 U.S.C. 103(a) as being unpatentable over Hardjono (US6584566B1) as applied to claims 1, 10, 19, and 28 above, and further in view of Koblitz and Srivastava (US6684331B1). In addition to the teachings applied above, while Hardjono fails to expressly disclose the mathematical relations involved in the steps for computing a first shared secret key and generating a first multicast group exchange key and steps for determining that a first departing member has left the second multicast group, selecting a private multicast group non-zero random integer, generating a second multicast group exchange key, broadcasting the second multicast group exchange key, computing a third secret key, and establishing a third multicast group, Koblitz teaches the mathematical relations in his

discussion of modular exponentiation by the repeated squaring method and the selecting step (Koblitz – page 23), Srivastava teaches the determining step (Srivastava – abstract), and the generating, broadcasting, computing, and establishing steps are a reapplication of four steps in Hardjono (abstract; column 3, lines 10-26; and figure 5, elements 505, 525, and 530). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify Hardjono by using the repeated squaring method to compute the first shared secret key and to generate a first multicast group exchange key and by including a selecting step as per the teachings of Koblitz, by including a step for determining that a first departing member has left the second multicast group as per the teaching of Srivastava, and by reapplying the generation, broadcast, computation, and establishment steps. One of ordinary skill in the art would have been motivated to do so in order to quickly create the keys in the computing and generating steps (Koblitz – page 23), to establish secure multicast communication (Srivastava – abstract), and to add a new member to the set of clients to whom data is multicast.

Conclusion

17. Any inquiry concerning this communication or earlier communications from the examiner should be directed to James Curcio whose telephone number is 703-305-8887. The examiner can normally be reached on Tuesday through Friday from 7:00 am – 5:30 pm.

18. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached at 703-305-1830. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

19. Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 703-305-3900.

JC
AU 2132
July 13, 2004

JUSTIN T. DARROW
PRIMARY EXAMINER